IPS Engine for FortiOS and FortiClient

Release Notes

VERSION 3.430

FORTINET DOCUMENT LIBRARY

http://docs.fortinet.com

FORTINET VIDEO LIBRARY

http://video.fortinet.com

FORTINET BLOG

https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT

https://support.fortinet.com

FORTIGATE COOKBOOK

http://cookbook.fortinet.com

FORTINET TRAINING SERVICES

http://www.fortinet.com/training

FORTIGUARD CENTER

http://www.fortiguard.com

END USER LICENSE AGREEMENT

http://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK

Email: techdocs@fortinet.com

IPS Engine - Release Notes

2017-08-30

43-340-443966-20170830

TABLE OF CONTENTS

Change Log

Date	Change Description
2017-08-30	Initial release.

Introduction

This document provides the following information for FortiOS IPS Engine version 3.430.

- What's New in IPS Engine 3.430
- Product Integration and Support
- Resolved Issues

For additional FortiOS documentation, see the Fortinet Document Library.

What's New in IPS Engine 3.430

Bug ID	Description
383197	Added support for OpenXML file detection.
391262	Fixed file filtering for .js files in ISNIFF.
398435	Support --skip-after and --quiet with custom signatures.
398524	Support --depend-on and --scan-range for custom application control signatures.
404123	Added support for VxLan tunnel decoding.
406203	Log certificate information from SSL/TLS traffic in Application Control log.
409661	Support RSA-PSS for ECDHE server key exchange.
412708	Added full TCP handshake packets to mirrored data sessions.
414642	Added support for SSL/TLS fragmented handshake message.
422891	Support Encapsulated Remote Switch Port Analyzer (ERSPAN). ERSPAN is based on GRE. By decoding ERSPAN in GRE tunnelling, we could detect the inner sessions from the mirrored/sniffered traffic. All ERSPAN frame types are supported, including I, II and III.
424433	Improved HTML obfuscation on Matching Condition of UTF Encode. The engine now detects the relevant UTF encoding by scanning the first 16-byte for Unicode encoded ASCII. This is mostly for exploits embedded in HTML/JS.

Bug ID	Description
434124	Support Internet Message Format (RFC5322). With this patch, the HTTP decoder can detect the content-type of "message/rfc822", and hand over to MIME decoder. The base64 decoder is also enhanced to support incremental update.
438617	Extended "--extract" option to support automatic number decoding. Now '*' can be used in the length field and 'auto' can be specified as the modifier so that the engine can auto detect the base of the number and convert to a numerical value. "--extract *,10,$1,auto; " tells the engine to detect a number at offset 10 and put the numerical value into register $1. Extended "--extract" option to support octal numbers. For example, "--extract 3,20,$8,oct;" tells engine to extract an octal number with 3 digits at offset 20 and put the value into register $8.

Product Integration and Support

Fortinet Product Support

The following table lists IPS engine product integration and support information:

FortiOS	5.2.0 and later 5.4.0 and later 5.6.0 and later
FortiClient	5.4.0 and later (Windows and Mac) 5.6.0 and later (Windows and Mac)

Resolved Issues

The resolved issues listed below do not list every bug that has been corrected with this release. For inquires about a particular bug, please contact Customer Service & Support.

FortiOS

General

Bug ID	Description
299327	Changed FortiView Session Accounting in sniffer and transparent mode by generating log messages statistics for long-live sessions and using the log messages to update report files.
386271	Fixed traffic delays of 30 seconds after running `execute update-ips` command.
383167	Fixed a random crash in Brotli decoder when traffic comes from proxy/WAD.
402010	Fixed IPS engine crash for tunnel traffic on Windows.
409184	Fixed out-of-order accounting which caused session bypass.
410227	Reduced long delay and high CPU usage that occurred when a large number of firewall policies with flow-based UTM are enabled.
411340	Support FSA inspection of URLs from email message body in SMTP traffic using sniffer Mode.
413661	Fixed the cause of IPS engine crash in build 309.
414835	Fixed partial SMB file submit for flow AV.
424099	Fixed IPS engine crash caused by libips.dll.
439158, 442976	Enhanced the custom rule loading process so that the rule loading loop cancontinue if invalid rule is detected.
443089	Fixed bug that triggered high memory usage by IPS engine and SSL traffic.
444237	Fixed IPS engine's high memory usage issue caused by SMB2 decoder.

Decoder

Bug ID	Description
377529	Improved Deep Application Control (DAC) performance when large number of concurrent engine processes are running, such as on high-end platforms.
393958	Fixed "Protect Server Mode" for RSA based key exchange when certificate/private key used on the FortiGate is different than the real server's key pair.
399319	Fixed TCP state transition to avoid false establishment of sessions, .
399973, 421455	Fixed suspicious code points in packet reassembler which could lead to packet accumulation.
403984	Fixed inaccurate traffic volume in sniffer traffic log.
404672	Fixed FP issue caused by TCP.Out.Of.Range.Timestamp. Timestamps will not be applied to PAWS check to RST packets. [RFC 1323]
407984, 408582, 408830	Fixed FTP decoder to properly track PUT/GET commands so that the relevant data transfer could be associated with the correct file names.
410268	Trigger Application Control deferred rule when a new application is matched.
423104	Fixed incorrect decoding of SNMPv2 trap.
434456	Fixed SSL session "failure to establish" bug that prevented traffic for certificate inspection from forwarding.

Flow AV

Bug ID	Description
394845	Mask off non-IPS/ Application Control features when no active Layer 7 decoders provide such features.
406913	Converted shared memory pool APIs to LMDB APIs for flowav virus url cache.

Signatures and Options

Bug ID	Description
408615	Fixed rule matching failure with CP8 for negative IP address matching.

Bug ID	Description
402773	Fixed incorrect custom application signature matching.
411374	Correctly copy all cross-session tags upon session creation.
445438	Don't explicitly release scan ranges on DB (re)load.

Inline SSL

Bug ID	Description
389591	Server did not detect EICAR virus with Internet Explorer. Fixed "Protect Server Mode" for RSA based key exchange when certificate/private key used on the FortiGate is different than the real server's key pair. Instead of entering dry run mode for RSA based key exchange, the engine now checks if the key pairs are the same. If they are not the same, the normal inline mode will be used.
406711	Support CRL verification for server certificate with an external service.
407506	Reset session ID in client hello to force full SSL handshake if the session ID cache lookup fails. This should avoid random unprocessed SSL sessions pass through which could lead to SSL errors.
422920	Fixed a race condition in SSL session ID cache lookup.
421697	Fixed a rare crash in ECDHE key exchange.

Webfilter and Flow AV

Bug ID	Description
401254	Preserve IPv6 flow label for FortiGuard URL filtering and Flow-AV.
408483	Flow-based static UR L Filter no longer blocking POST request when combined with Flow-AV. For exempted URLs, both FortiGuard URL rating and URL filtering in subsequent packets should be exempted as well.
421050	Fixed a bug that resulted in websites being blocked when the Flow-AV is enabled and Web Filter and Application Control security profiles were applied to a policy.
439159	Fixed block page generation for HTTPS URL filtering with certificate inspection. .

Bug ID	Description
442976	Enhanced the custom rule loading process to fix a bug that caused flow-based web filtering to fail due to improper regex entry.

FortiClient

Bug ID	Description
424099	Fixed a bug where libips.dll caused fortiws.exe to crash and improved error logs.
441349	Fixed FortiEsNac handle leak in Windows.
441674	Fixed a bug that caused fortifws.exe process to crash.
444628	Fixed a problem that led to connection issues for Windows 8 / 10 machines.

FORTINET®

High Performance Network Security